neustar
Real Intelligence. Better Decisions.

Security-Related Information

Monitoring, Staffing, and Processes

Preventative and predictive maintenance routines are performed weekly, monthly and/or annually based on manufacturer recommendations and Industry best practices Mechanical and Electrical system reactive and routine maintenance activities are performed using established Neustar processes and notification procedures as required. **Our continual forecast trending and analysis of capacities provide insight for predictive maintenance and future installation requirements.** Data Center personnel use Neustar cabling and labeling standards that have been developed using Industry best practices and then adapted for our unique applications and designs. We employ the use of a separate "build room" for testing, installing OS, and "burn in" of equipment before it hits the data center floor to reduce the potential for early equipment lifetime failures in production.

The Neustar Difference

Neustar has honed our competency across all areas within the Layer—data center location, security, internal mechanical, electrical, and fire suppression systems, staffing, and processes—to meet/exceed the specific requirements of the NPAC/SMS through our many years of actual operation of the U.S. LNPA service. Security-Related Informatic

As shown in Exhibit 1.2.1-2, Neustar's NPAC/SMS Security-Related Information has a proven, audited track record of exceeding and far exceeding Industry-best practices. Neustar's data centers continue to score well above "Industry Best Practices" and in many cases are best in class as highlighted in our 2012 annual operations audit (required by the NPAC Master Agreement) completed by a neutral third-party auditor. In addition, Neustar data centers are included in scope for numerous audits including Sarbanes-Oxley (SOX) and SSAE16 (formerly SAS70) without issue.

Data Center Environment–Article 14 Audit Scores

Category	2008	2012	Trend
Data Center Environment Overall	**4.60**	**4.67**	▲
Physical Space	4.40	4.40	⟷
General	4.20	4.20	⟷
Racks and Placement	4.50	4.50	⟷
Division of Space	4.20	4.20	⟷
Labeling and Marking	4.60	4.60	⟷
Documentation	4.50	4.50	⟷
Electrical Elements	4.50	4.70	▲
Backup Power Sources	5.00	5.00	⟷
HVAC and Air Handling	4.80	4.90	▲
Smoke Detection	4.80	4.80	⟷
Fire Protection	4.80	4.80	⟷
Water Detection	4.80	4.80	⟷
Facilities Modification	4.50	4.50	⟷
Facilities Inspection	4.80	4.80	⟷

5 - Excellent performance, far exceeds industry best practices
4 - Above average performance, generally exceeds industry best practices
3 - Average performance, meets industry best practices
2 - Below average performance, fails to meet industry best practices
1 - Poor performance, falls far below industry best practices

005.npac2013

Exhibit 1.2.1-2: Third-party audits validate our performance and provide valuable input on possible future enhancements.

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

new

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

SeSecurity-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

Network Infrastructure–Article 14 Audit Scores

Category	2009	2012	Trend
Network Architecture	**4.70**	**4.73**	▲
Documentation	4.70	4.70	⟷
Documentation Maintenance	4.50	4.50	⟷
Public Addresses	4.80	4.80	⟷
Private Addresses	4.90	4.90	⟷
IP Addresses Requests	4.80	4.80	⟷
DNS Architecture	4.60	4.60	⟷
Internet and Customer Connectivity	4.80	4.80	⟷
Network Monitoring	4.90	4.90	⟷
Handling Failures	4.60	4.60	⟷
High Availability	**4.60**	**4.68**	▲
WAN Access	4.60	4.60	⟷
Firewalls	[redacted]		⟷
VPN Concentrators	5.00	5.00	⟷
Routers and Router/Switches	4.60	4.70	▲
IOS/Hardware and Maintenance	**4.70**	**4.70**	⟷
IOS	4.60	4.60	⟷
Testing	4.60	4.60	⟷
Change Control	5.00	5.00	⟷
Out-of-Band Management	4.70	4.70	⟷
Emergency Maintenance	4.60	4.60	⟷
Hardware Inventory	4.50	4.70	▲
Ticketing Systems at Neustar	4.70	4.70	⟷
Customer Notification	4.50	4.70	▲

5 - Excellent performance, far exceeds industry best practices
4 - Above average performance, generally exceeds industry best practices
3 - Average performance, meets industry best practices
2 - Below average performance, fails to meet industry best practices
1 - Poor performance, falls far below industry best practices

006.npac2013

Exhibit 1.2.1-5: **Third-party audits validate our performance and provide vauable input on possible future enhancements.**

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

The Neustar Difference

While the hardware described here is dedicated exclusively to the NPAC service, the exact same types of hardware are used for other applications within Neustar. This affords us extensive experience with these components outside of the NPAC operational environment. Consequently, our technical staff is well trained and very familiar with all the hardware components within the NPAC environment. All changes to NPAC infrastructure are first implemented within a different operational Neustar service. This way, changes are validated in a production environment before they are brought to the NPAC.

1.2.1.3.2 Four Layers of the NPAC/SMS Application Software

The NPAC/SMS Application is a very large and complex repository of application code. To help manage this complexity, the software itself is broken into the four different layers. Each layer provides a particular service or functionality within the system. Each layer is built on top of the previous layer.

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

new

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

1.2.1.3.3 Ensuring High Availability of the NPAC/SMS

The NPAC/SMS is a high availability system, consistently operating at or above 99.9% availability over the past 5 years. At the application level, several architectural and functional aspects contribute to this availability:

1. **Multi-Process, Multi-Machine Architecture**—This architecture means that, in most cases, if a process stops or if even an entire machine stops, the system continues to run.
2. Security-Related Information
3. **Process Management**—This feature provides NPAC/SMS-specific automated oversight of all processes, restarting a process if it ever stops. The use of shared memory allows the NPAC/SMS to retain important information that otherwise would have been lost when the process stopped.
4. Security-Related Information

Security-Related Information

1.2.1.3.4 NPAC/SMS Special Features

While the primary function of the NPAC/SMS is to manage information related to telephone numbers, the system offers a wide array of functionality that both complements basic transactions and improves the quality of the overall ecosystem. What follows is a brief overview of these features.

Synchronization

One of the most important functions of the NPAC/SMS is to ensure the local systems are in synch with the NPAC/SMS data. The integrity of the U.S. communications network relies on all SPs having the same addressing information, at the same time in order to properly route voice calls as well as SMS/MMS messages. To this end, the NPAC/SMS provides many different mechanisms to ensure synchronization among all communications SPs.

- Security-Related Information

- **Bulk Data Download (BDD)**—These files provide local systems the ability to re-create or update their databases based on data extracts taken from the NPAC/SMS. BDD files are available for all types of NPAC data (SV, pooled block, network data, Service Provider, notifications). These files can be generated based on activity in a certain timeframe, or for the entire database.

- **Automated Resend**—During overnight hours, the NPAC/SMS looks for local systems that are still on the failed list for SVs or pooled blocks and resends the downloads of these objects. We designed this feature to examine previous failure reasons and if the error indicates that a modify download was failed because the record does not exist in the local system, the NPAC will broadcast a Create operation rather than a download.

- **Audits**—The NPAC/SMS queries the LSMS systems for a specified set of telephone numbers, and compares the responses to its own data. Discrepancies are noted in an audit report, and corrective downloads are sent to any discrepant LSMS systems.

Mass Update/Mass Port

Service Providers often have a need to port large volumes of numbers in a controlled manner but require assistance to manage this process. The mass update/mass port tool was developed to provide this assistance. Mass update/mass port transactions can be defined for all types of NPAC/SMS operations (create, release, activate, modify, disconnect, and cancel).

Many options are available to control the execution of the job, including an ability to control the start time and to suppress notifications that normally would be generated. Several types of reports are available to monitor the progress and results of each job.

The mass update/mass port subsystem uses a scheduler process and a system of quotas to ensure all work is done in a fair and orderly fashion at reasonable volumes. The broadcast quota system is quite complex, and considers the following aspects when running "jobs".

- Whether the job will produce SV downloads, Pooled Block downloads, or no downloads at all
- The hour of the day the job is running;
- The day of the week the job is running; and
- Whether the job is being run by a provider or NPAC personnel.

The mass update/mass port subsystem also includes a dashboard that allows administrators to determine available broadcast quota and view projected completion times for jobs.

Optional Fields

Over time, the Industry has been interested in adding new types of data to the NPAC. However, this was a difficult process, largely because changes to the CMIP interface required many resources for development and testing.

To address this issue, Neustar developed the concept of optional fields. With this feature, a one-time change to the CMIP interface was made to add a new string to several of the existing CMIP messages. This string takes the form of an Security-Related Information that conforms to an Industry-approved schema that defines additional data fields. With this mechanism, a new field can be added to the NPAC without changing the CMIP interface definition.

The implementation of these fields in the NPAC is done dynamically, such that adding a new field requires minimal development and can be implemented during a maintenance window.

Pseudo-LRN

Pseudo-LRN (pLRN) provides a mechanism to add records to the NPAC that do not have an LRN associated with it. By using a specially tagged LRN value, these records are identified as pLRN and are broadcast only to systems that have opted in to receive pLRN records. Providers can opt in to all pseudo-LRN records or only for pseudo-LRN records from a certain set of providers.

OpGUI

The NPAC/SMS is a very complicated system that can process millions of requests in a single day. Many of these requests have service level requirements that must be met to fulfill the expectations of our customers. Management of this system could prove to be a challenge, but Neustar has built an infrastructure that has allowed the NPAC administrators to successfully manage the system for many years. This infrastructure includes an administrative interface, called the OpGUI, which provides functionality required to configure and maintain the NPAC/SMS. The OpGUI provides the following functionality for a system administrator to manage the NPAC/SMS:

1. **Managing NPAC Customer Profiles**—provides the capability to add, remove and modify NPAC Customers, configure their tunable options, configure their CMIP network access, and establish service bureau relationships.

2. **System Administrator Reports**—provides system administrators the ability to generate reports for needed to manage and tune the NPAC/SMS.

3. **Mass Update/Mass Porting (MUMP) Management**—provides system administrators the capability to manage all mass update and mass porting jobs that Service Providers ask the NPAC to perform on their behalf. These functions include creating, removing and updating MUMP jobs, projects, quotas, and profiles, as well as generating MUMP reports.

4. Security-Related Information

5. **User Administration**—allows NPAC administrators to add, remove, and update accounts that grant access to the NPAC OpGUI.

6. **System Parameter Management**—allows NPAC administrators to view and update the hundreds of system level parameters provided by the NPAC/SMS.

7. **CMIP Gateway Configuration**—allows NPAC administrators to configure the processes that provide the NPAC CMIP interface. These functions include assigning provider's systems to specific CMIP gateway processes and managing the parameters associated with the CMIP gateway.

8. **Billing Collection Configuration**—allows NPAC administrators to configure the information that is collected by the NPAC/SMS for billing purposes.

In addition to the OpGUI, Neustar has also built tools that provide a real-time view into what each NPAC region is processing and how well it is handling the load. Among these tools is the Security-Rele that provides a detail view into the Dispatcher Module that directs the messaging for a region. From this tool an administrator can see all messages being routed through the system and what process is working the request. Each request received by the NPAC/SMS may pass through as many as four processes. It's necessary to understand this traffic flow to ensure the NPAC/SMS is meeting the service level requirements associated with response time and SOA/LSMS interface performance.

Another administrative tool Neustar has built is the Security-Related Information This tool provides a real-time cross-regional display of the key metrics related to NPAC/SMS performance and reliability. The Security-Re provides two columns of metrics for each NPAC region. There is a metric delta column and a metric cumulative column for each of the following key metrics.

- Monthly, daily, and five-minute SLR 3 pass, failed, and percentage passed
- Monthly SLRs 5 and 6 pass, failed, and percentage passed
- Partial failure counts for subscription versions
- Database performance including average query, rollback, and commit times
- Count of SOA or LSMS systems in recovery
- Rules engine processing active and backlog queues
- CMIP interface active queue for each SOA/LSMS
- Count of long running requests
- Machine load for the application server machines
- Count of running NPAC/SMS processes

Another key feature that contributes to our successful management of the NPAC/SMS is the multitude of **dynamically configurable settings** that control system behavior. Neustar engineers have developed this capability to make it easier to manage the multitude of options offered by the NPAC/SMS, as well as, to easily extend the service for new functionality. Settings can be defined at several different levels, including at the interface level, at the provider level, and at the overall system level. For example, we can configure the duration of medium timers at the system level, but also configure whether a particular SOA supports medium timers. The NPAC/SMS has more than